CERT-In Advisory CIAD-2021-0004

Preventing Data Breaches / Data leaks (TLP: WHITE)

Original Issue Date: January 20, 2021

Severity Rating: High

Description

It has been observed that incidents of data breach and data leaks affecting Indian organisations are on the rise. In cases of data breaches, the main targets of attackers are businesses, financial institutions, healthcare sector, e-commerce, and startups. The kind of information usually targeted is data that can identify particular individuals such as email, mobile no, medical reports etc., organisation's trade secrets and/or intellectual property (IP).

Attackers are using a variety of techniques to overcome the security systems of their targeted businesses in order to steal private data. They try to target public-facing/external systems of businesses to ultimately gain access to the internal networks, servers and databases.

Another trend which has been observed is that attackers are exfiltrating data and then deploying ransomware to encrypt the data they have stolen. In such incidents, attackers also threaten to release the stolen data in public domain, if the ransom is not paid.

I. Common causes of Data breach / Data leak

The common causes of such incidents are as follows:

Misconfiguration

Poorly configured network devices can inadvertently allow traffic that would otherwise have been blocked, while incorrect file permissions on a server could expose vital data to risk. It is also possible to send data accidentally to any wrong person, misconfigured servers and careless uploads to public folders, directory listing can also lead to data breach or leakage.

Application Vulnerabilities

Application vulnerabilities are system flaws or weaknesses in applications that could be exploited by threat actors to compromise the security and integrity of the application.

Insider Threat

Most insider misuse happens through misinformed / uninformed staff and disgruntled /compromised users. Although most data breaches are facilitated by external malicious actors, it is still the case that insiders with or without privileged access are playing a key role in data breaches. People make mistakes and their minor mistakes could lead to a big loss to the business. Confidential information may get distributed without using any data prevention techniques.

Weak/ Default/ Stolen Credentials

Stolen or default credentials are one of the easiest ways attackers get access to systems, enabling them to gain access to sensitive content and resources. Also poorly configured VPN and Work from Home methods result in compromise of legitimate accounts and further misuse.

II. Best practices to prevent data breaches:

i. Organisations are advised to prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)

ii. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

iii. People have always been the weakest link in the cybersecurity chain. Provide training to employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they shouldn't to use their corporate device- especially in Work from Home environments.

iv. Establish and maintain an incident response team and evaluate incident response plans frequently.

v. Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest. Deploy data loss prevention (DLP) solutions / processes.

vi. Deploy detection and alerting tools and create process to prevent, contain and respond to a data breach/ data leak.

vii. Develop and maintain strong policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA). MFA adds additional layer of security and reduces the risk of perpetrator using stolen credentials to move an attack further.

viii. Always keep up-to-date operating systems and other application software because attackers identify the bugs in old versions and use them to attack.

ix. Consider using models that take the `least privilege' approach to provide security for both on-and off-premises resources (i.e. zero-trust models). Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a

network perimeter.

x. Micro-segmentation helps contain the movement by giving organizations increased control over lateral communication that occurs between resources. Furthermore, in the event of a breach, micro-segmentation serves to limit the possible lateral exploration of networks by bad actors.

xi. Enforce BYOD security policies, like requiring all devices to use a business-grade VPN service and antivirus protection.

xii. Create policies and plans for engaging with governance, risk management and compliance teams.

xiii. Evolve and implement a Data Backup policy. All the business critical data should be backed up regularly to prevent data loss and to ensure faster recovery from data breach.

III. Best Practices while using Amazon's AWS S3 and EC2 services:

Data breach/data leak incidents have involved compromise or mis-configured AWS S3 and EC2 instances. Best practices for preventing such incidents while using Amazon AWS S3 and EC2 services are given below:

i. Check public accessibility of all AWS instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.

ii. Ensure proper security of AWS access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.

iii. Implement appropriate security measures for testing, staging and backup environments hosted on AWS. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.

iv. It must be noted that Amazon's Cloud services follow a model wherein a number of security aspects are customer's responsibility. It is advised to be thoroughly aware of these and implement appropriate security policies and controls. Following are a list of resources which may be diligently studied and suggested measures may be implemented as appropriate to infrastructure and environment.

- Introduction to AWS Security whitepaper
  https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
- Amazon S3 Security
  https://docs.aws.amazon.com/AmazonS3/latest/dev/security.html
- AWS Security Best Practices whitepaper
  https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
- AWS Security Best Practices Checklist
  https://totalcloudio.medium.com/security-best-practices-checklist-a23274c726cd

IV. Best practices while using MongoDB and Elasticsearch servers:

It has been observed that data breach/leakage incidents have involved MongoDB and Elasticsearch instances also. Major factor in all such incidents has been observed to be a lack of appropriate authentication mechanism and proper security measures allowing unauthenticated remote attackers to access and manipulate the databases.

Best practices for securing MongoDB:

i. Enable Role-based access control to enforce authentication and require users to identify themselves.

ii. Use TLS/SSL for all incoming and outgoing connections including communication between internal components of MongoDB as well as between applications and MongoDB.

iii. Encrypt the MongoDB data stored in the storage layer and use appropriate file system permissions to restrict access to the data.

iv. Use firewalls to minimize overall exposure and ensure that only traffic from trusted sources can reach the system running MongoDB and that MongoDB can only connect to trusted outputs.

Best practices for securing ELK stack instance:

i. Use a reverse proxy software such as nginx or mod_proxy (for Apache HTTP server) to restrict direct access to the ELK components and configure it properly to have Role-based access control.

ii. Change the default ports of Elasticsearch, Logstash and Kibana on which connections are made.

iii. Use firewalls to restrict connections to the system running the ELK stack. Please refer CERT-In advisory CIAD-2019-0017 "Securing MongoDB and ELK stack instances" for detailed account of best practices.

V. Steps to be taken when organisation/entity is affected by a data breach/data leak:

i. Disconnect the compromised system from the internet, but don't turn it off. Turning of the system could result in loss of crucial evidences which would be needed for the analysis and investigation of the incident.

ii. Ensure all credentials in an organization, including service accounts, are reset and that default passwords or those similar to previous passwords are not used.

iii. Report the data breach/ data leak to CERT-In Incident Response Help Desk immediately. (email: incident AT cert-in.org.in , see Contact us page for details)

iv. Notify users/customers who could be affected immediately with details of information breached; actions being undertaken to address the problem and how they can reach back for any queries.

VI. Best practices for individual users to safeguard against data breaches

i. Use strong and unique passwords for all the online accounts. Use a password manager software. Use different passwords for different online accounts.

ii. Enable two-factor authentication wherever available.

iii. Regularly update all the software on computers, smartphones and other devices. Install a reputed anti-virus solution on systems, keep it updated and configure it to run scans periodically.

iv. Be vary of clicking links received in unsolicited SMS messages or emails. Do not open email attachments from unknown senders. Limit sharing personal information on public online forums.

v. While making online payments, ensure that the merchant website as well as the payment gateway websites are running on HTTPS and have a valid certificate (usually shown as a "green lock" symbol near the address bar in most browsers).

vi. Do not share personal information, OTPs etc. over phone calls purporting to come from customer service, bank etc. Refuse to install any apps on smartphone / computer if asked to do so by an unknown person over phone call or in person.

vii. Refer to website https://www.cyberswachhtakendra.gov.in for security best practices and free bot removal tools for computers and mobile devices.

References

https://www.computerworld.com/article/3535590/avoid-security-breaches-how-to-protect-your-data.html
https://its.ucsc.edu/security/breaches.html
https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/security-of-the-aws-infrastructure.html
https://www.mongodb.com/security-best-practices
https://dev.to/ndaidong/how-to-make-your-mongodb-container-more-secure-1646
https://logz.io/learn/complete-guide-elk-stack/#use-cases
https://www.infosecawareness.in/home/index.php
https://www.cyberswachhtakendra.gov.in/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India